МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

КРЕМЕНЧУЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

ІМЕНІ МИХАЙЛА ОСТРОГРАДСЬКОГО

КАФЕДРА АВТОМАТИЗАЦІЇ ТА ІНФОРМАЦІЙНИХ СИСТЕМ

ЗВІТ

ЗВІТ З ЛАБОРАТОРНИХ РОБІТ

З НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

**«ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ»**

Виконав студент групи КН-23-1

Полинько Ігор Миколайович

Перевірив: ассистент кафедри АІС Андреєв П. І.

Кременчук 2025

**ЛАБОРАТОРНА РОБОТА № 3**

**Тема:** Шифрування методом Вернама

**Мета:** навчитися писати програми для шифрування (дешифрування)

методом Вернама

**Порядок виконання роботи:**

Розробити програмний код застосування бібліотеки шифрування даних методом Вернама. При цьому:

Змоделювати кодер з послідовністю ключів із 17 елементів.

**Варіант: 15**

**Скрипт програми:**

import random  
  
KEY\_LENGTH = 17  
key = [random.randint(0, 255) for \_ in range(KEY\_LENGTH)]  
print("Згенерований ключ (17 елементів):", key)  
  
plaintext = input("Введіть текст для шифрування: ")  
  
plain\_bytes = plaintext.encode("utf-8")  
  
cipher\_bytes = bytearray()  
for i, byte in enumerate(plain\_bytes):  
 cipher\_byte = byte ^ key[i % KEY\_LENGTH]  
 cipher\_bytes.append(cipher\_byte)  
  
cipher\_hex = cipher\_bytes.hex()  
print("\nШифртекст (у hex):", cipher\_hex)

**Результат:**

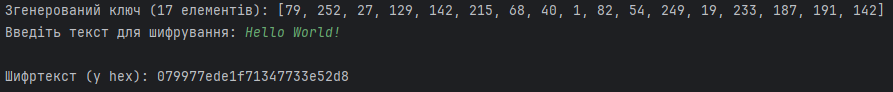
****

Рисунок 3.1 – Результат шифрування програми

**Висновок:** на цій лабораторній роботі ми навчилися писати програми для шифрування (дешифрування) методом Вернама.

**Контрольні питання:**

1. **Що таке шифрування, дешифрування?**
   1. Шифрування – це процес перетворення відкритого тексту у зашифрований, щоб зробити його незрозумілим для сторонніх.
   2. Дешифрування – це зворотний процес: перетворення зашифрованого тексту назад у початковий, зрозумілий вигляд.
   * У шифруванні завжди беруть участь два основні елементи: повідомлення (що шифрується) і ключ (за допомогою якого воно шифрується).
2. **Що таке алфавіт, текст?**
   1. Алфавіт – це множина всіх можливих символів, які можуть входити до тексту.
   * Наприклад: для англійського тексту – A–Z, a–z, пробіл, пунктуація тощо.
   * Для комп’ютера алфавіт – це просто набір чисел (байтів) від 0 до 255, бо будь-який символ має свій код у таблиці ASCII або UTF-8.
   1. Текст – це послідовність символів із певного алфавіту.
   * У нашому випадку ми кодуємо його в байти, щоб виконувати математичні операції над ними.
3. **Що таке ключ:\?**
   * Ключ – це секретна послідовність даних, за допомогою якої виконується шифрування та дешифрування.
   * Без правильного ключа отримати початковий текст практично неможливо.
   * У нашому прикладі ключ – це набір випадкових чисел від 0 до 255, який ми генеруємо ось так:
   * key = [random.randint(0, 255) for \_ in range(17)]
4. **У чому полягає шифрування методом Вернама?**
   1. Кожен байт відкритого тексту XOR’иться (тобто додається за модулем 2) із байтом ключа.
   2. Формула:
   3. y = x ⊕ k

де

x – байт відкритого тексту,

k – байт ключа,

⊕ – операція XOR (виключне "АБО"),

y – байт зашифрованого тексту.

* + Якщо виконати ту ж саму операцію ще раз, то ми отримаємо початковий байт:
  + (x ⊕ k) ⊕ k = x

Тобто XOR сам себе «знищує» при повторному застосуванні.

* + Ідея: якщо ключ абсолютно випадковий і ніколи не повторюється, такий шифр неможливо зламати – це ідеально стійке шифрування.

1. **Як можна реалізувати нескінченну послідовність ключів?**
   * Один із способів – повторювати ключ циклічно, як у нашому коді:
   * key[i % KEY\_LENGTH]

Тобто якщо текст довший за ключ, програма починає використовувати ключ заново з початку.

* + Інший спосіб – генерувати ключ динамічно, наприклад, із генератора псевдовипадкових чисел (PRNG), який видає нескінченну послідовність байтів.

1. **Яким має бути текст перед безпосереднім шифруванням?**

Текст повинен бути:

* + - перетворений у байти (через .encode("utf-8")),
    - без «сирих» символів, які не входять до алфавіту (наприклад, нечитабельні юнікодні знаки без підтримки у шифрі),
    - чітко визначений – без додаткових пробілів або невидимих символів, щоб результат був відтворюваним.